ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE

Paper ID #37155

An Undergraduate Research Experience in Unmanned Aircraft Systems (UAS) Cybersecurity – Outcomes and Lessons Learned

Matthew A. Verleger (Professor of Engineering Fundamentals)

Matthew Verleger is a Professor of Engineering Fundamentals at Embry-Riddle Aeronautical University. He received his PhD in Engineering Education from Purdue University in 2010. His research interests include student use of models and modeling, flipped-classroom environments, development of educational software, and gamification of engineering courses.

Richard Stansbury (Associate Professor)

Mustafa Ilhan Akbas (Assistant Professor)

An Undergraduate Research Experience in Unmanned Aircraft Systems (UAS) Cybersecurity – Outcomes and Lessons Learned

Abstract

This paper is an update of a Work-in-Progress presented at the ASEE 2021 virtual conference [1] and includes new data from after the 2021 paper was accepted for publication. An undergraduate research experience was developed in response to an Office of Naval Research program seeking to develop "innovative solutions that directly maintain, or cultivate a diverse, world-class STEM workforce in order to maintain the U.S. Navy and Marine Corps' technological superiority." During the fall 2020 semester, nine students were recruited to participate in a UAS cybersecurity-focused undergraduate research experience. Three faculty members each identified a small topic area for undergraduate students to pursue. The three areas are:

1. Small UAS (sUAS) Vulnerability and Threat Assessment and Mitigation
2. Effects of Cyber Attacks on Communication in UAS Swarms with Distributed Swarm Control
3. Enhancing Security of Cloud-Connected UAS Services

Students were placed onto teams based on their prior course experiences and the project requirements. Common resources were provided for all students to train them in conducting research. Teams were then tasked with developing a more comprehensive research plan for their specific project and carrying out that plan throughout the 2020-2021 academic year. A no-cost extension was granted to enable six students who had not graduated to continue into the Fall 2021 semester with the goals of completing their work and publishing the results in an academic outlet. Three students continued into the Spring 2022 semester finishing their publication work.

Year 1 of the program was assessed by having students take a pre-, mid-, and post- survey and conducting a brief interview about their experiences. Students took a pre-survey at the start of the project and a mid-project survey shortly before the winter break. They completed the post survey and interview during the final week of the Spring semester in Year 1. Five students who remained with the project in Year 2 also completed a "final year" survey at the end of the Fall term in year 2. The surveys were a combination of project specific skills questions as well as relevant questions from the Undergraduate Research Student Self-Assessment (URSSA), an NSF funded assessment tool to measure student gains in research skills.

This paper will describe the broader project, the individual student team projects and the outcomes of those projects, and results from the surveys and interviews. The purpose of this paper is to provide an example approach for future undergraduate research programs looking for practical approaches to implementing undergraduate research programs, particularly those in the cybersecurity area.

Introduction

In 2013 Jeff Bezos announced on the TV program 60 Minutes that Amazon wanted to deliver packages via "drones," which at the time sounded ludicrous. In August 2020, the Federal Aviation

Administration (FAA) approved Amazon’s use of drones for package delivery. According to the FAA, the number of recreational drones in the U.S. is predicted to peak at around 1.5 million, and the number of commercial drones is expected to double by 2024. With a massive increase in civilian and commercial use of drones (also called unmanned aircraft systems or UAS), cybersecurity has become a topic of great concern, as they are essentially “flying computers,” containing much of the same components as laptops and smartphones, such as CPU and RAM, high-resolution cameras, WiFi, GPS, as well as a host of other sensors. Particularly concerning to the U.S. government is that most commercial off-the-shelf (COTS) UAS are manufactured by Chinese companies, such as DJI, who holds as much as 75% market share of an $21 billion per year industry. The cybersecurity implications of this led the U.S. Department of Defense (DoD) to ban the purchase and use of COTS UASs for DoD work in 2018, and the following year the U.S. Department of the Interior grounded its fleet of 70 DJI UASs. Accordingly, there has been an increased interest in how to secure UASs.

Project Overview

This project took place at a medium-sized, business-and-STEM only institution in the south-eastern U.S. Sponsored by the Office of Naval Research (ONR), the intended purpose of this project is to develop “innovative solutions that directly maintain, or cultivate a diverse, world-class STEM workforce in order to maintain the U.S. Navy and Marine Corps' technological superiority.”[2] The project team accordingly developed a paid undergraduate research experience for students to participate in throughout the academic year exploring research in cyber-security related topics. Nine (9) students were recruited into the program and divided into three project teams of three students each based on a brief interest survey and their respective backgrounds. The three projects are described in Table 1.

Table 1. UAS Project Descriptions

Project #1 - Simulated Effects of Non-Ideal Physical and Cybersecurity Conditions on UAV Swarming

This research project utilizes two simulation software tools to model traveling swarms of unmanned aerial vehicles (UAVs) connected in an unmanned aerial system (UAS) and aims to provide an interactive software where users can create a model of a UAV swarm and subject it to possible stimuli. The simulated swarms can be subject to disconnections due to physical barriers, cyberattacks, or network failures.

This research project considers the use of UAS in what can be described as “non-ideal” conditions or environments. An environment for a UAS is defined as “non-ideal” if it reduces the overall effectiveness by limiting the communication and maneuver capabilities. UAVs experience a myriad of issues when placed in challenging environments. These issues such as communication loss and uplink/downlink failures would only be amplified in operations of one or more UAS. Utilization of modeling software helps simulating difficult conditions.
The simulation tool, NetLogo 3D [3], is used to simulate the formation and movement of the UAV swarm due to its vast movement modeling capabilities and user-friendly interface. The alignment of the swarm is based on the boid model designed to simulate the fluid movement of bird flocks [4]. All agents generated begin with an urge to the center of the three-dimensional

field and an urge to the closest agents within a pre-defined radius. The agents are placed at random points and are drawn to the center point by the central urge. The agents pass the center point and adjust according to their urges to other agents. The agents continue to move around the three-dimensional field together as a swarm and maintain the formation with minor adjustments. The cyberattack function in the NetLogo model shuts down one agent in the swarm at random, causing it to separate from the swarm and immediately drop from to the ground. The swarm continues to function correctly as the inactive drone lacks any of the urges of the active drones and is not recognized by the surrounding agents as a member of the swarm.

NS3 is a discrete-event network simulator for internet systems [5]. Its full simulation of the UAS communication is utilized to account for real conditions such as latency, and packet loss. UDP is used to send datagrams between UAV nodes to coordinate the formation of a swarm. Understanding the risk that a malicious UAV poses to the swarm with realistic communication conditions in a military application is essential. For this purpose, we implemented APAWSAN [6], [7] swarming algorithm, which is based on virtual forces. We simulated a cyber-attack in which a peripheral UAV is compromised. Its function is altered to deceive the network into thinking it is also a central node. The mean absolute deviation of position between the central node and the other nodes only increases with time and the swarm never reaches a proper formation. This poses a significant risk for swarms that use virtual forces without packet verification, or another form of cryptography which prevents attackers from tampering with messages. Our demonstration shows that controlling a single node in the swarm allows an attacker to wreak havoc on the entire swarm.

Project #2 – Small UAS (sUAS) Vulnerability and Threat Assessment and Mitigation

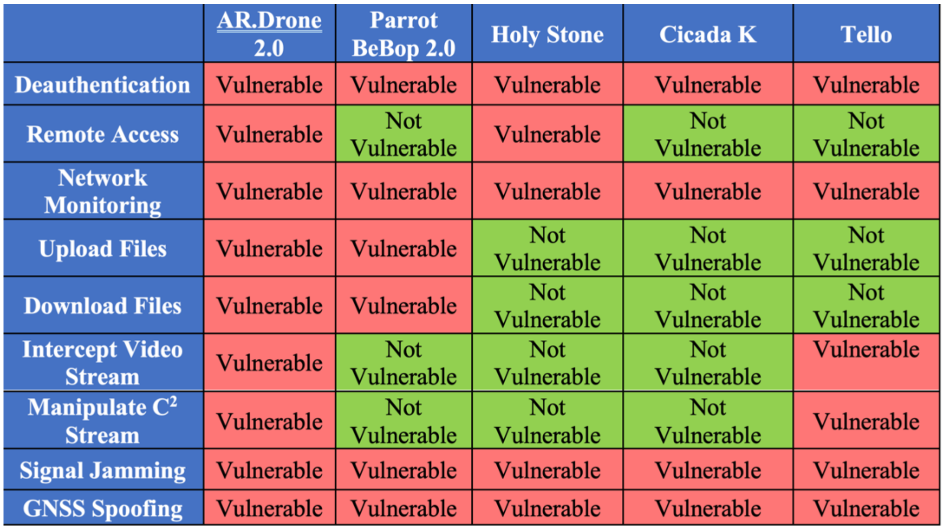
Commercial off-the-shelf drones (COTS) are essentially flying computers, and are evolving technologies that are relatively inexpensive, improving at a dramatic rate, and widely available throughout the world. Threat actors, including insurgents, terrorists, and extremist organizations have used these drones in conducting offensive attacks, as wells as for developing battlefield situation awareness. Technological improvements combined with their availability requires enhanced and adaptive countermeasures to enhance battlefield awareness and to protect the warfighter. COTS drones, unlike military-grade drones, have been demonstrated to have cyber-related vulnerabilities that can be exploited to render these drones ineffectual, harmless, or at a minimum, cause degraded performance.

For this project students were provided with several COTS drones and tasked with identifying known cybersecurity vulnerabilities, as well as conducting original research to identify new vulnerabilities. The students used standard cybersecurity tools and techniques to identify these vulnerabilities. Afterward, the team applied several quantitative measures of risk and vulnerability that are commonly used in the cybersecurity world to identify the criticality of cybersecurity vulnerabilities. These included:

- STRIDE model [8]: a threat model developed by Microsoft to aid in identifying common threats to a computer system. STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service, and escalation of privileges

- DREAD model [9]: DREAD stands for damage potential, reproducibility, exploitability, affected users, and discoverability. DREAD is usually used in conjunction with threat models as DREAD scores an attack based off the impact and likelihood of the event; this severity analysis paired with threat analysis that comes with STRIDE is what makes up risk assessments.
- CVSS [10]: The Common Vulnerability Scoring System, also known as CVSS, is an open framework for communicating qualities and severity of software vulnerabilities in quantitative form. CVSS has three types of scores: *base*, *temporal*, and *environmental*. A base score represents the qualities of a vulnerability that are constant over time and across environments; a temporal score represents the qualities that change over time; and an environmental score represents the qualities that are unique to a user's environment.

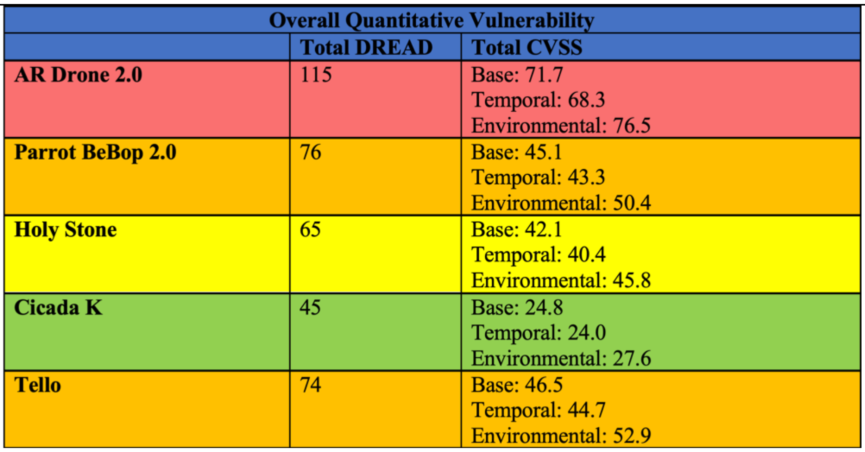
As shown in Table 2, all COTS drones investigated evidenced several cybersecurity vulnerabilities. Note that all drones were susceptible to some attacks (jamming) and is expected. Drones using Wi-Fi for command, control, and communications were susceptible to deauthentication attacks, due to how the Wi-Fi protocol functions.



	AR.Drone 2.0	Parrot BeBop 2.0	Holy Stone	Cicada K	Tello
Deauthentication	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Remote Access	Vulnerable	Not Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable
Network Monitoring	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Upload Files	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Download Files	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Intercept Video Stream	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Vulnerable
Manipulate C^2 Stream	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Vulnerable
Signal Jamming	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
GNSS Spoofing	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable

Table 2. Results of vulnerability research

Table 3 summarizes overall quantitative vulnerability scores, demonstrating the relative vulnerability for each drone.



Overall Quantitative Vulnerability		
	Total DREAD	**Total CVSS**
AR Drone 2.0	115	Base: 71.7 Temporal: 68.3 Environmental: 76.5
Parrot BeBop 2.0	76	Base: 45.1 Temporal: 43.3 Environmental: 50.4
Holy Stone	65	Base: 42.1 Temporal: 40.4 Environmental: 45.8
Cicada K	45	Base: 24.8 Temporal: 24.0 Environmental: 27.6
Tello	74	Base: 46.5 Temporal: 44.7 Environmental: 52.9

Table 3. Overall quantitative vulnerability scores

Project #3 - Blockchain for UAS Cloud Connectivity

Across civilian and defense mission sets, UAS collect, process, and distribute a tremendous volume of information. To enable the scalability of UAS communications, the introduction of cloud resources has provided the opportunity to implement multiple resources to receive, process, store, validate, and retransmit to other Command, Control, Communication, Computing, and Intelligence (C4I) systems. Such system must ensure the confidentiality, integrity, and availability of the data transmitted within the network.

To address these challenges, the team sought to implement a blockchain-enabled communication and computing architecture. Figure 1 illustrates the architecture in which one or multiple UAS operate to perform a mission. Telemetry and sensor data are communicated to the Ground Control Station (GCS). The GCS shall transmit its data to a local edge computing server. Each time new data has been received or existing data modified, the change shall be stored in the blockchain ledger. The blockchain ledge ensures the integrity of the transmitted data blocks through the ledger's cryptographic hashing of the received data. With sufficient cloud resources, the availability of the data can increase as more nodes can store the data with its integrity assured. Confidentiality shall be maintained by using a private block chain.

The team selected and used the Ethereum General Purpose Blockchain [11]. For the edge server, the team implemented a client to write GPS telemetry received from the GCS to the blockchain, to retrieve data on the blockchain, or to append to current blockchain files. The edge server writes the blockchain recorded data elements to the cloud via Web3J [12] and JSP [13] to an AWS cloud instance running Lambda [14]. The team successfully demonstrated the architecture transmitting UAS telemetry from a simulated UAS via Microsoft AirSIM [15].

The team successfully implemented the proposed architecture; however, did not complete the experiments necessary to demonstrate confidentiality, integrity, and availability improvements.

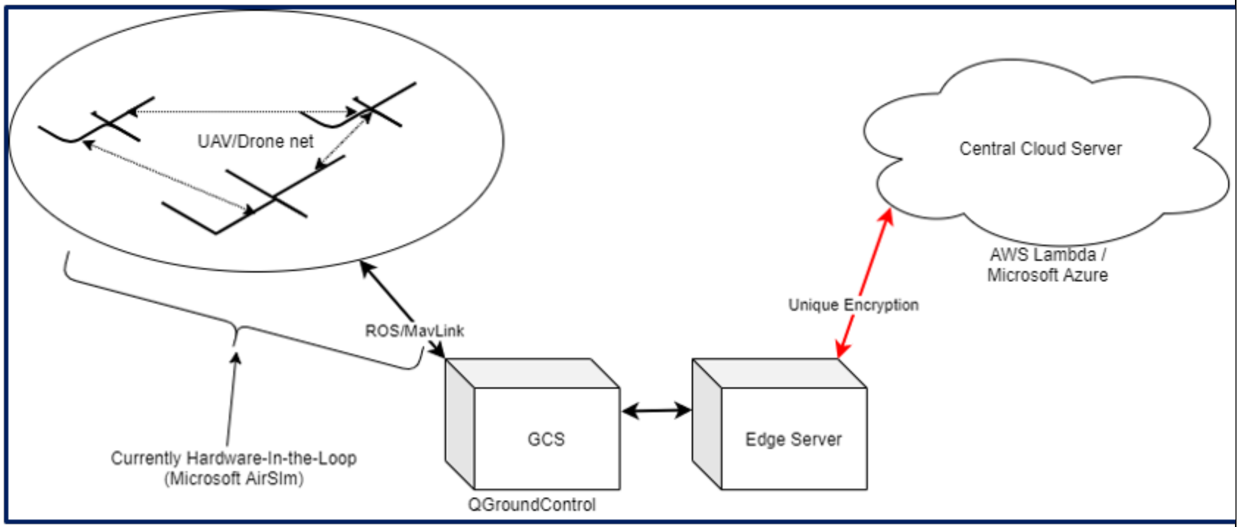


Figure 1. Notional Architecture for Blockchain for UAS Cloud Connectivity

Each project was identified and led by a faculty member who mentored their project team through the research process. A graduate student oversaw all three teams and helped coordinate and address any ongoing issues.

Participants

Nine (9) students were recruited with the following demographic characteristics:

- Seven male, two female
- Seven White, two Black or African American
- Three of Hispanic, Latino, or Spanish origin
- Four computer science majors, one software engineering major, two homeland security majors, and two unmanned aircraft systems majors
- One Freshman, four Juniors, and four Seniors
- The average cumulative GPA was 3.46 with a range from 3.274-3.771
- Seven ROTC participants, two non-ROTC participants
- None of the students had participated in non-course related research during the academic year prior to this research
- 1 student had participated in non-course related research during the summer

While ONR sponsored the program and preferred students to also be participating in ROTC, there was no requirement that students be affiliated with the military. Students were recruited in late August and early September via email from the ROTC commanders, departmental communications in cyber-security focused majors (specifically, computer science and homeland security), and personal invitations from the project PIs to former students. Students completed a brief application describing their background and verifying that they meet ONR's participation requirements. All applicants met the requirements, and no applicants were rejected from the program.

Program Implementation

Student teams were given a general focus area with guidance from their faculty advisor. Throughout the fall, student teams focused on refining those focus areas toward specific research questions through a literature search. The deliverable for the fall term was a project proposal and presentation to the entire project cohort and representatives from ONR describing the research questions and the research plan the team had developed to address those questions. In the Spring term, teams worked to carry out their proposal and provide a presentation on the results. Like the fall, the presentation was to both the project cohort and ONR representatives.

In addition to the two (2) end-of-term presentations, there were also all-hands meetings held monthly throughout project where teams would update the cohort on their progress. This gave all project participants an opportunity to better understand the work their colleagues were doing and ask clarifying questions to help build a stronger end-of-term presentation.

For the 2nd year of the project, six (6) students returned to work in the Fall 2021 semester on their projects again. The focus for Year 2 was on identifying an appropriate publication outlet and preparing a manuscript for publication. An end-of-term presentation was given outlining any changes in the project outcomes and discussing the manuscript venue and purpose. Of the six students, three (3) returned in the Spring 2022 term to finalize their manuscripts.

Data Collection

Participants completed up to four surveys throughout the project. The instruments were based on the URSSA [16], [17], as well as a few project-specific evaluation questions related to students knowledge of cybersecurity topics. At the end of Year 1, students also participated in semi-structured interviewed about their experience. Table 4 shows the data collection timeline and number of responses received.

Table 4. Data Collection

Instrument	Timeline	Number of Responses
Pre-Survey	August 2020	9
Mid-Project Survey	December 2020	9
Year 1 Survey	April 2021	8
Year 1 Interviews	April 2021	8
Year 2 Survey	December 2021/January 2022	6

The survey consisted of 89 Likert-style items and 7 open-ended response questions, with only minor wording changes to reflect timing of the survey in relation to the project. Responses were matched across each survey for analysis, though with only 9 responses, no statistical analysis was conducted. The Year 1 Survey is included in the Appendix. Questions were divided into 6 categories shown in Table 5.

Table 5. Survey Question Groupings

#	Response Options	Category
21	Never heard of it, Heard of it, but I don't know anything about it, Minimal knowledge, Basic introductory knowledge, Moderate knowledge, Expert/Advanced knowledge	Project Specific Skills
37	Not at all, Just a little, Somewhat, A lot, A great deal	Knowledge and Skills with Research
6	Yes, Somewhat Yes, Somewhat No, No	Interest in Scientific Communication
5	Strongly Agree, Agree, Disagree, Strongly Disagree	Expectations from experience
7	Very Likely, Likely, Unlikely, Very Unlikely	Future career/education plans
11	Yes, No	Reason(s) for participation
2	1-7 (Highly Dissatisfied to Highly Satisfied)	Overall Satisfaction

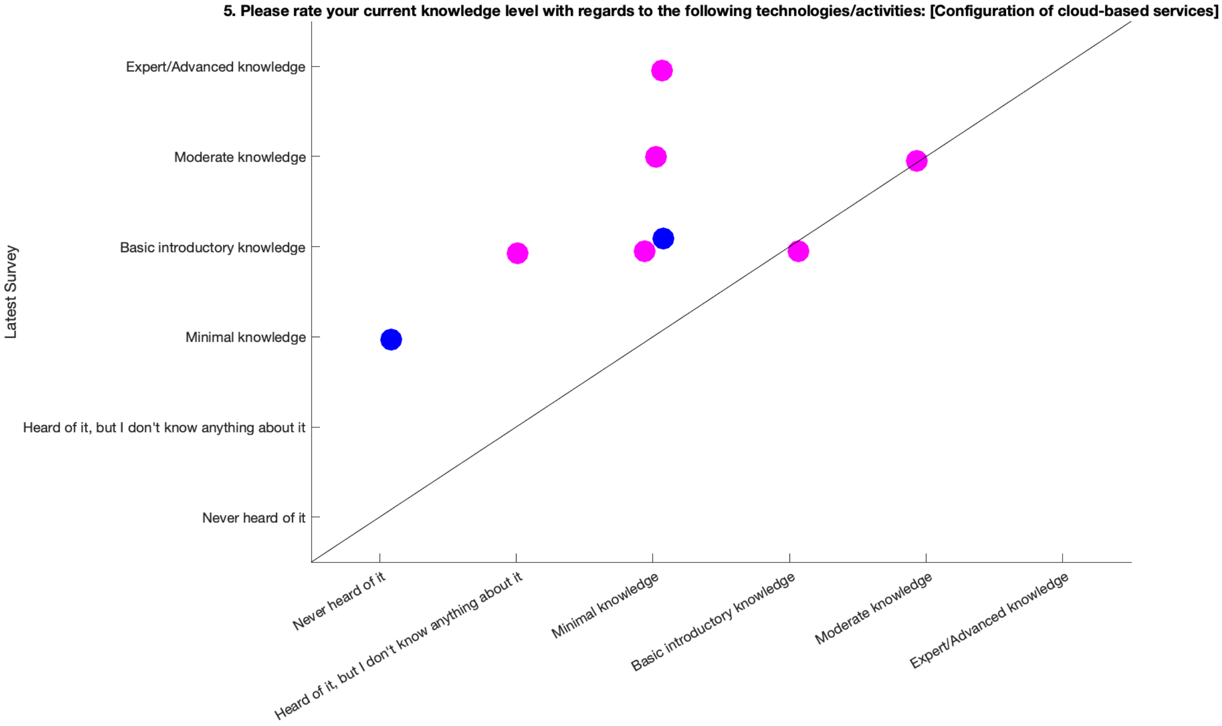
Analysis

Of the original 9 participants, 1 student completed only the pre- and mid-project surveys, disengaging from the project in the middle of the Spring term. Two (2) students completed the pre-, mid-, and Year-1 surveys and six (6) completed all 4 iterations of the survey. Graphs were generated to show the change in response between the pre-survey to the latest survey a participant completed. A small amount of random noise was added to the numerical values assigned to each response to enable co-located responses to be differentiated. Responses were also color-coded to show if the latest response comes from the mid-project survey (green), end-of-year-1 survey (blue), or end-of-year-2 survey (magenta).

Project Specific Skills

Due to an error on the pre-survey, the experience with the project-specific skills were not captured until the mid-project survey. Analysis for this section looked at the mid-project survey to the latest survey completed. As one student did not respond to the surveys beyond the mid-project survey, their data was removed from this portion of the analysis. Within this section, most students showed small to moderate improvement in their self-evaluative knowledge of the various items.

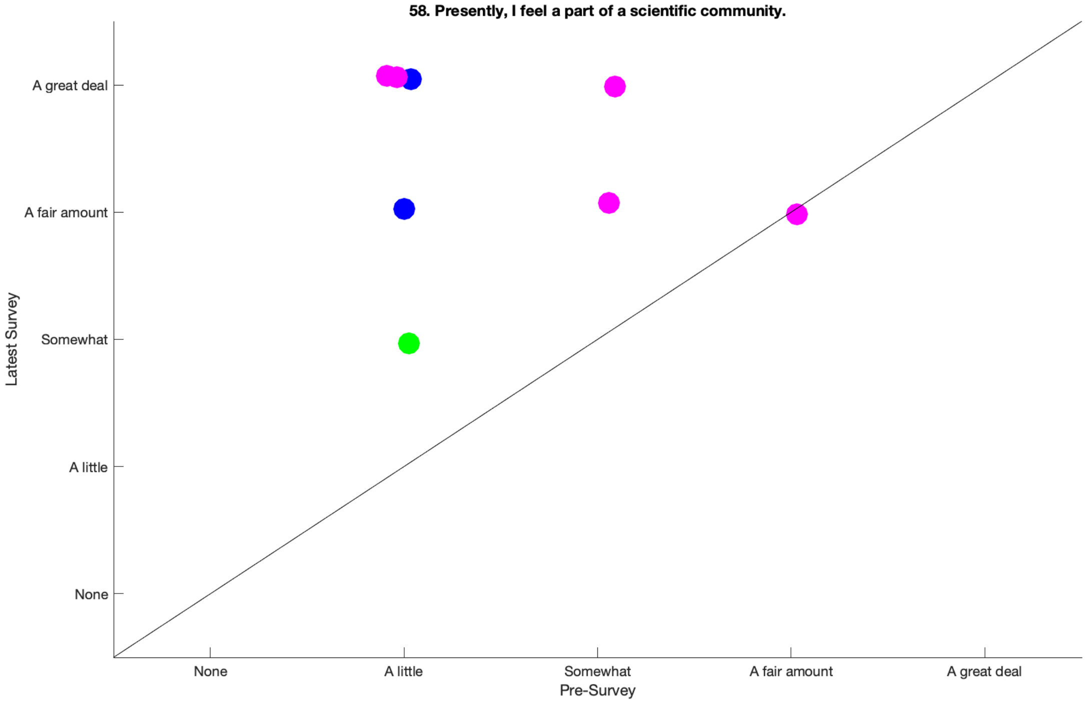
Of particular interest were the responses regarding their knowledge of “Configuration of cloud-based services”. While students in project #3, which actively used cloud computing, would be expected to have more experience than those in the other projects, it was interesting to see small amounts of improvement in three other students as well. During one of the team presentations, project #3’s team did discuss some of the issues they were having with setting up the cloud infrastructure and the benefits and challenges of using that infrastructure.



Knowledge and Skills with Research

In examining the survey results for this section, the majority of responses show improvements as expected – small to moderate gains for most students in nearly every skill queried. One item of particular interest that appeared throughout the responses from the individual who disengaged from the project during the middle of the Spring term. They only completed the pre- and mid-surveys, that occurred at the beginning and end of the Fall term when the majority of research was focused on literature review and proposal development. Of the 37 items in this category, this student rated themselves as only improving their research skills and knowledge on 5 of them, while their skills decreased on 21 items. This decrease in their perceived skill could have been an early indicator of their disengagement. They did not participate in the interview process, so their reason for disengaging is not known, but future implementations should be more purposeful in reviewing this aggregate change in responses and identifying that this student clearly was not getting benefits from the work in the same way as their peers.

Perhaps the most important outcome from this section is in regards to the question of "Presently, I feel a part of the scientific community", where 8 of the 9 respondents indicated an increase.



Interest in Scientific Communication

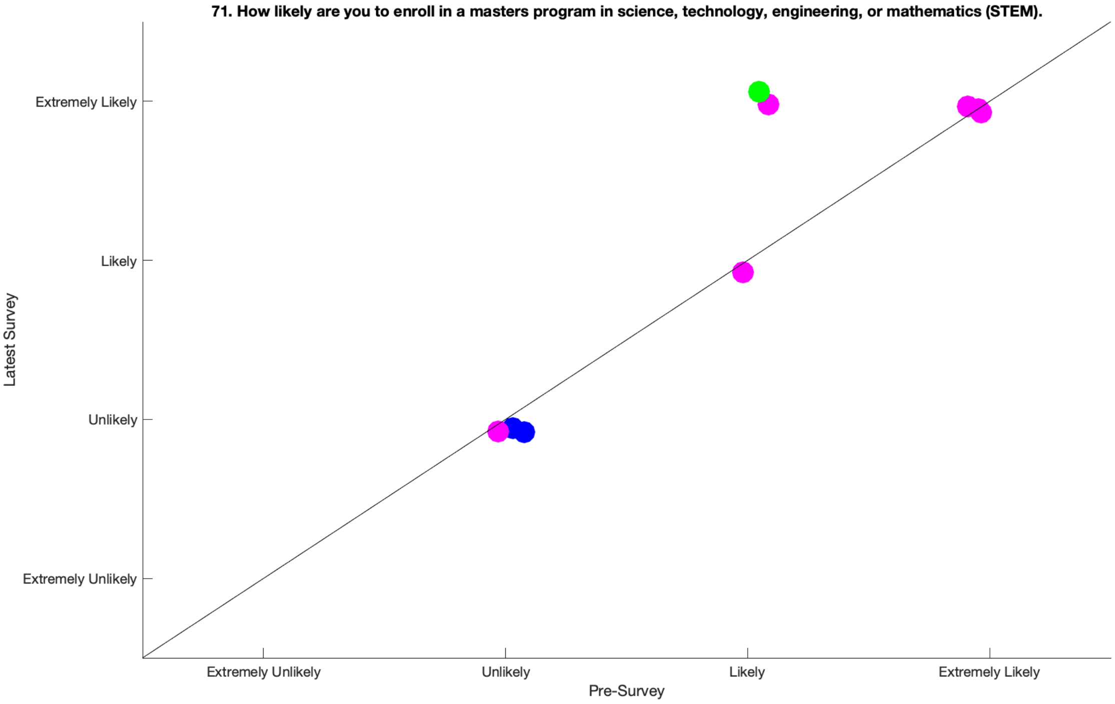
This portion of the survey asked participants about their desire to participate in various forms of scientific communication. One clear trend is that students' desire (or lack of desire) to participate in scientific communication was the same, regardless of the type of communication. If a student was interested in one form (e.g., presenting a talk or poster at a professional conference), they were nearly equally interested in all forms (e.g., publishing in a journal). Only 1 student had any variation on this trend, actively working on a talk/poster for a professional conference and a journal publication, but they did not want to attend a professional conference. Of the 8 participants who responded to both the pre- and end-of-year-1 surveys, 7 of them showed increasing interest in scientific communication over time.

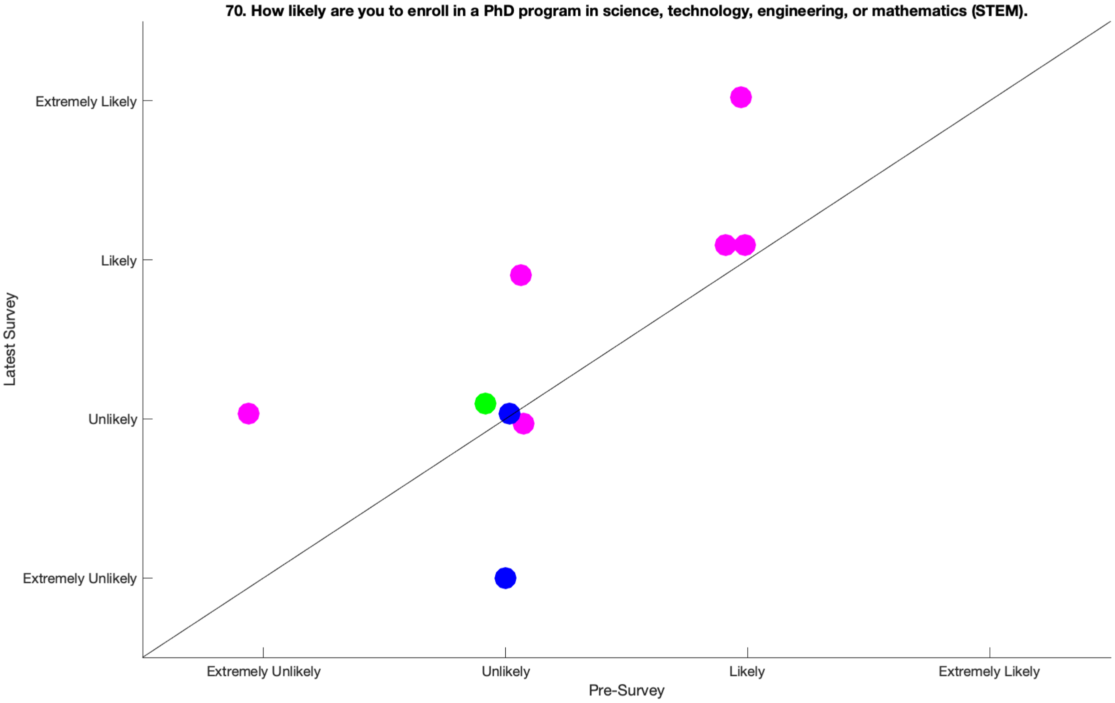
Expectations from experience

Participation in an undergraduate research experience should be a formative experience that better prepares participants for their future endeavors. When asked, there was 100% agreement across all 4 surveys that students expected their relationship with their academic and career interests to benefit from participation in the program.

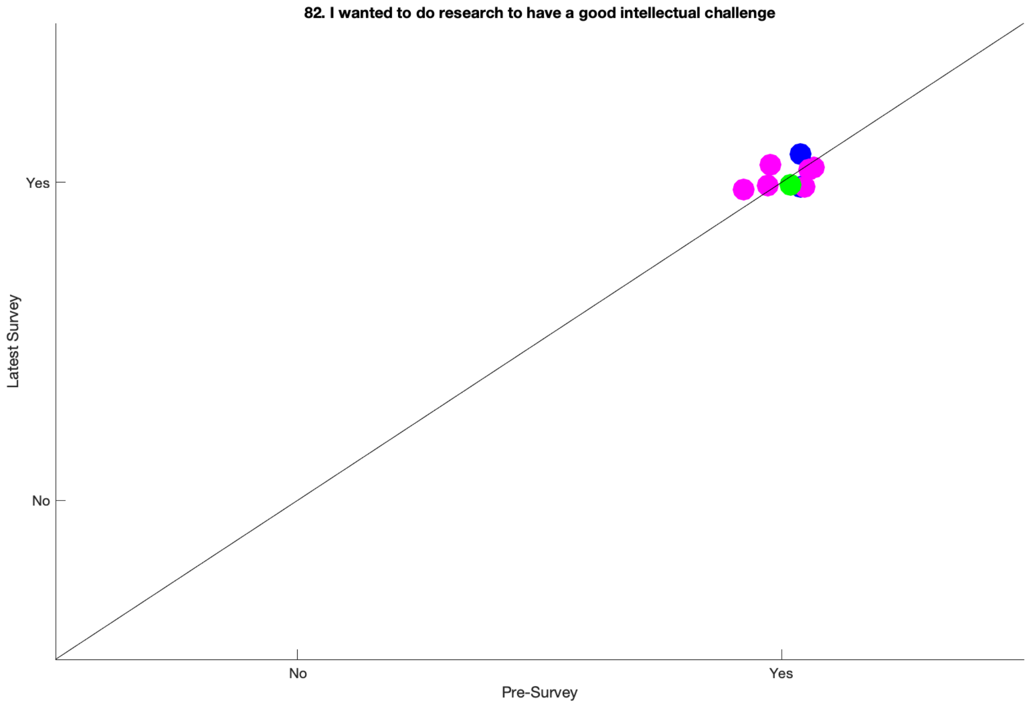
Future career/education plans

As expected, participation in the program had a small positive impact on students' interest in pursuing a STEM masters degree. Less expected was the increased interest in pursuing a PhD in a STEM program. The increased interest in graduate work was also not a function of enrollment in ROTC. Of the 9 participants in the program, 7 of them were in ROTC programs which include some degree of post-undergraduate military commitment which could impact their graduate school options. The two non-ROTC students did not show any increased interest.





Reason(s) for participation



While there was some variability in responses to the other reasons for participating, the intellectual challenge was nearly always a core driver of all of the students to participate. Only twice did a student say that the intellectual challenge was not a reason for participating, but their perspective had changed by the final survey.

Overall Satisfaction

On average, students rated the overall program 6.375/7.0 and the mentors 7.0/7.0 in their final survey response.

Interviews

The interview process revealed three key findings. First, the value of the literature review in the research process. Almost every student mentioned the literature review in their interview, however Manuel captured it best when he said “I think I see the value of doing a lot of literature review in a sense of trying to tie back the research you’re finding, the conclusions you’re coming to, tying it back to a whole ‘why is this important’…”. The first semester of the project focused almost exclusively on reviewing the literature and generating a research proposal. This strong emphasis on the literature was clearly an impactful decision.

The second finding was in the value of having a graduate student mentor to oversee all three projects in addition to the individual project faculty mentors. According to Ethan, “It was interesting because the meetings we would have with (the graduate student)… I wouldn’t say it was less professionalism, but because he was a fellow students, it was nice." While there were regular meetings between the project teams and the faculty mentors, multiple students commented on the added value of having a more senior student they could engage with as a way of providing a more accessibility to the research. They felt less concerned about how they were perceived by the graduate student and better empowered to ask "dumb" questions that would ultimately benefit the research.

Finally, the program had an unexpected benefit in its focus on ROTC students. Megan described how she "… didn't get a chance to do an internship or anything with my summer training schedule… it gave me some work experience… more of a professional level instead of just the classroom setting." By participating in the program throughout the academic year, she was able to gain skills that would otherwise not have been available to her because of her summer ROTC commitments.

Conclusions and Future Work

This project aimed to increase student understanding of research and cyber-security topics and based on the student responses to the surveys, interviews, and the publications being produced, appears to be successful in achieving that aim. The self-reported understanding of research topics were generally favorable and students felt meaningfully engaged in their respective research projects. This paper highlights that the overall project demonstrated success throughout the program and that the small-group approach used could be successful for other programs seeking to implement more undergraduate research programs.

The following recommendations are for individuals considering the development of an undergraduate research experience:

1. Consider seeking out participants in ROTC or other groups who may not be able to participate in more traditional summer experiences (i.e., internships, co-ops, etc.).
2. Include a strong focus on the literature review phase of research. While literature review is rarely the most enjoyable part of conducting research, it is nevertheless foundational to understanding the research process.
3. Regularly gather as a full cohort to discuss each team's project. While the individual project teams were deeply invested in their own project, there was also some benefit to having teams hear about the process and challenges their peers were going through in the other projects.
4. Consider adding a graduate student or senior undergraduate mentor to the program as an additional support pathway for students as they engage in their project.
5. Consider, where possible, funding projects long enough to generate publications from the project. While it was not in the original funding cycle, because of how the program had to adapt to COVID, funding was available for each project team to produce a publication on their work, further demonstrating the research cycle. This would not have been possible under our original design, but had been a productive outcome of this project and given the participants a more complete research experience.

Acknowledgments

This work relates to Department of Navy award N00014-20-1-2515 issued by the Office of Naval Research. The United States Government has a royalty-free license throughout the world in all copyrightable material contained herein.

References

[1] M. A. Verleger, R. S. Stansbury, M. I. Akbas, and P. Craiger, "Work in Progress: Developing Undergraduate Research Experiences in Unmanned Aircraft Systems (UAS) Cybersecurity," presented at the 2021 ASEE Virtual Annual Conference Content Access, Jul. 2021. Accessed: Jan. 18, 2022. [Online]. Available: https://peer.asee.org/work-in-progress-developing-undergraduate-research-experiences-in-unmanned-aircraft-systems-uas-cybersecurity

[2] Office of Naval Research, "ONR FOA Announcement # N00014-19-S-F009 FY19 Funding Opportunity Announcement (FOA) for the Office of Naval Research (ONR) Navy ROTC Cybersecurity Training Program," 2020.

[3] S. Tisue and U. Wilensky, "NetLogo: A Simple Environment for Modeling Complexity," May 2004, vol. 21, pp. 16–21.

[4] "Flocks, herds and schools: A distributed behavioral model | Proceedings of the 14th annual conference on Computer graphics and interactive techniques." https://dl.acm.org/doi/abs/10.1145/37401.37406?casa_token=YRAdTpi5APYAAAAA:o62FG5Vaycz_xk-GILkr5qyAH9yQvUR8OcMocDbU__6rOMeITe1mYW3jQ03ibo6ajz59gH5SNxe0Zw (accessed Feb. 03, 2022).

[5] G. Carneiro, "NS-3: Network simulator 3," in *UTM Lab Meeting April*, 2010, vol. 20, pp. 4–5.

[6] M. İ. Akbaş and D. Turgut, "APAWSAN: Actor positioning for aerial wireless sensor and actor networks," in *2011 IEEE 36th Conference on Local Computer Networks*, Oct. 2011, pp. 563–570. doi: 10.1109/LCN.2011.6115518.

[7] J. Rentrope and M. I. Akbaş, "Spatially Adaptive Positioning for Molecular Geometry Inspired Aerial Networks," in *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, New York, NY, USA, Nov. 2017, pp. 1–8. doi: 10.1145/3132340.3132348.

[8] L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Interface Microsoft Corp.*, vol. 33, 1999.

[9] H. Michael and L. David, "Writing secure code." Microsoft Press, 2002.

[10] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," *IEEE Secur. Priv.*, vol. 4, no. 6, pp. 85–89, Nov. 2006, doi: 10.1109/MSP.2006.145.

[11] "Home," *ethereum.org*. https://ethereum.org (accessed Feb. 03, 2022).

[12] "web3j - Lightweight Ethereum Java and Android integration library." http://web3j.io/ (accessed Feb. 03, 2022).

[13] W. Beaton, "Jakarta Server Pages," *projects.eclipse.org*, May 10, 2018. https://projects.eclipse.org/projects/ee4j.jsp (accessed Feb. 03, 2022).

[14] "Serverless Computing - AWS Lambda - Amazon Web Services," *Amazon Web Services, Inc.* https://aws.amazon.com/lambda/ (accessed Feb. 03, 2022).

[15] *Welcome to AirSim*. Microsoft, 2022. Accessed: Feb. 03, 2022. [Online]. Available: https://github.com/microsoft/AirSim

[16] University of Colorado Boulder, “Evaluation Tools: Undergraduate Research Student Self-Assessment (URSSA).” https://www.colorado.edu/eer/research-areas/undergraduate-research/evaluation-tools-undergraduate-research-student-self (accessed Feb. 15, 2021).

[17] T. J. Weston and S. L. Laursen, “The Undergraduate Research Student Self-Assessment (URSSA): Validation for Use in Program Evaluation,” *CBE—Life Sci. Educ.*, vol. 14, no. 3, p. ar33, Sep. 2015, doi: 10.1187/cbe.14-11-0206.

Appendix – Year 1 Survey

1. **Please rate your current knowledge level with regards to the following technologies/activities:**

	Never heard of it	Heard of it, but I don't know anything about it	Minimal knowledge	Basic introductory knowledge	Moderate knowledge	Expert/Advanced knowledge
Linux Operating System						
Java						
Python						
Cloud-based Services						
Configuration of cloud-based services						
Pixhawk Autopilot						
PX4						
Cybersecurity: Data Privacy						
Cybersecurity: Data Integrity						
Cybersecurity: Risk Mitigation						
Cybersecurity: Threat Assessment						
Cybersecurity: Threat Detection						
Cybersecurity: Threat Response						
Port scanning						
Vulnerability analysis						
Device Intrusion						
UAS Swarming						
Agent Based Simulation						
Communication Network Simulation						
Commercial Off the Shelf Small Unmanned Aircraft System Swarms (COTS sUASs)						
Anti-drone counter measures						

2. **Presently I understand...**

	A great deal	A lot	Somewhat	Just a little	Not at all	Not applicable
how to analyze data for patterns.						
how to figure out the next step in a research project.						
problem-solving in general.						
how to formulate a research question that can be answered with data.						
how identify limitations of research methods and designs.						
the theory and concepts guiding my research project.						
the connections among scientific disciplines.						
the relevance of research to my coursework.						

3. **Presently, I am...**

	A great deal	A lot	Somewhat	Just a little	Not at all	Not applicable
confident in my ability to contribute to science.						
comfortable in discussing scientific concepts with others.						
comfortable in working collaboratively with others.						
confident in my ability to do well in future cyber-security related courses.						
able to work independently.						
patient with the slow pace of research.						
understanding of what everyday research work is like.						
taking great care in conducting procedures in the lab or field.						

4. **Presently, I can...**

	A great deal	A lot	Somewhat	Just a little	Not at all	Not applicable
Write scientific reports or papers.						
Make oral presentations.						
Defend an argument when asked questions.						
Explain scientific concepts to non-scientists.						
Prepare a scientific poster.						
Keep a detailed lab notebook.						
Conduct observations in the lab or field.						
Use statistics to analyze data.						
Calibrate instruments needed for measurements.						
Work with computers.						
Understand journal articles.						
Conduct database searches or scholarly internet searches.						
Manage my time.						

5. **Presently, I...**

	None	A little	Some	A fair amount	A great deal	Not Applicable
can engage in real-world scientific research.						
feel like a scientist.						
think creatively about the project.						
can try out new ideas or procedures on my own.						
feel responsible for the project.						
work extra hours because I am excited about the research.						
interact with scientists from outside your school.						
feel a part of a scientific community.						

6. **As part of this research experience, I would like to...**

	Yes	Somewhat yes	Somewhat no	No
present a talk to other students or faculty.				
present a talk or poster at a profession conference.				
attend a conference.				
write or co-write a paper that will be published in an academic journal.				
write or co-write a paper that will be published in an undergraduate research journal.				
win an award or scholarship based on my research.				

7. **As part of this research experience, I expect that this research will...**

	Strongly Agree	Agree	Disagree	Strongly Disagree
confirm my interest in my field of study.				
clarify for me which field of study I want to pursue.				
prepare me for advanced coursework or thesis work.				
prepare me for graduate school.				
prepare me for a job.				

8. **How likely are you to...**

	Extremely Likely	Likely	Unlikely	Extremely Unlikely
enroll in a PhD program in science, technology, engineering, or mathematics (STEM).				
enroll in a masters program in science, technology, engineering, or mathematics (STEM).				
enroll in medical or dental school.				
enroll in a non-STEM PhD program.				
enroll in a non-STEM masters program.				
enroll in a program to earn a different professional degree (i.e., law, veterinary medicine, etc.).				
pursue certification as a teacher.				

9. In 2-3 sentences, describe your current career goals for after graduation:

10. In 1-2 sentences, how did you first learn about the research program?

11. I wanted to do research to:

	Yes	No
explore my interest in science		
gain hands-on experience in research		
clarify which field I wanted to study		
clarify whether graduate school would be a good choice for me		
clarify whether I wanted to pursue a science research career		
have a good intellectual challenge		
work more closely with a particular faculty member		
participate in a program with strong reputation		
get good letters of recommendation		
enhance my resume		
earn some money		

12. Are there any other reasons you chose to participate in this research:

13. In 1-2 sentences, describe the project you are currently working on:

14. In 2-3 sentences, describe the work you have personally done on this project.

15. In 2-3 sentences, describe what work you would still like to do on the project if it were to continue.

16. How satisfied are you with your project and the work you are doing for it?

Highly Dissatisfied						Highly Satisfied
1	2	3	4	5	6	7

17. How satisfied are you with the mentorship that your faculty mentor is providing your team?

Highly Dissatisfied						Highly Satisfied
1	2	3	4	5	6	7

18. How could your faculty mentor better enable your team for success?

19. In 1-2 sentences, describe any special actions your team has had to take to work on your project because of the COVID-19 pandemic beyond the general precautions required by the university.